UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,388	08/16/2007	Mark Nadim Olivier De Clercq	NL04 0156 US1	8723

65913 7590 02/27/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
02/27/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/590,388	DE CLERCQ, MARK NADIM OLIVIER	
	Examiner	Art Unit	
	LONGBIT CHAI	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2009*.

2a)☒ This action is FINAL. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1 – 20.

Response to Arguments

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment.

3. As per claim 1 and 10, Applicant remarks the prior-art does not teach the amended claim limitation "wherein the data signal convey protected information". Examiner respectfully disagrees because Laackmann teaches (a) for security-relevant circuits, the reverse engineering should be prevented such as preventing an erase of the data held in a memory chip upon the removal of the material that surrounds or covers the semiconductor chip since the passivation layer of the chip is, generally, accessible (e.g., via probing) (Laackmann: Para [0039] Line 9 – 13, Para[0004] Line 1 – 5 and Para [0003] Line 15 – 18) (b) Examiner notes the protected data from erasing in the memory chip where the memory chip must comprise data / address buses to another part of electronic circuits that comprises a part of the connection means arranged for transferring data signals (i.e. as to be protected data) between those two electronic circuits; besides, (c) as per another connection means where the data signal conveyed on Figure 1 is also qualified as protected information since Laackmann teaches the signal receiver must receive approximately identical signal values from the transmitter (Para [0046]) and hence the conveyed signal level / information is normally protected unless an intrusion attack alters the signal value by changing the associated capacitance value.

4. As per claim 3, Applicant remarks the prior-art does not teach performing any storage functions. Examiner respectfully disagrees because Laackmann teaches the memory chip as

one side of electronic circuits (Laackmann: Para [0039] Line 9 – 13, Para [0004] Line 1 – 5 and Para [0003] Line 15 – 18), which, Examiner notes, must comprise a storage element such as part of the transistors as the component element of a chip that comprise the buffering circuits to buffer / store data-bit signal.

5. As per claim 4 and 6, Applicant remarks the prior-art does not actually measure capacitance. Examiner respectfully disagrees because (a) Laackmann teaches the reverse engineering of a semiconductor chip can be prevented by detecting the change of capacitance as a change of part of connections means (Laackmann: Para [0005], Para [0039] Line 9 – 13, Para [0004] Line 1 – 5 and Para [0003] Line 15 – 18) and (b) by electronic theory, one does not need to actually measure capacitance since the characteristics of a capacitance can be measured / detected from a set of other electrical parameters (e.g., time constant associated with a capacitance) which may then cause a signal receiver receives non-identical signal value from a signal transmitter.

6. As per claim 7, Applicant remarks the prior-art does not teach deriving a reference signal from a Monte-Carlo analysis. Examiner respectfully disagrees because Rayane teaches a Monte-Carlo analysis is carried out to computer the variation of measurement due to tolerance – i.e. Examiner notes the expected measurement value (i.e. reference signal value) needs to consider the acceptable tolerance via the Monte-Carlo simulation (Rayane: Section 1 & 4.1).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed

in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1 – 3, 6, 8 – 10 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Laackmann et al. (U.S. Patent 2003/0132777).

As per claim 1 and 10, Laackmann teaches an electronic device for cryptographic processing, comprising:

at least two electronic circuits coupled via a connection means, wherein the connection means is arranged for transferring data signals between the two electronic circuits, wherein the data signal convey protected information (Laackmann: Para [0039] Line 9 – 13, Para[0004] Line 1 – 5, Para [0003] Line 15 – 18 and Para [0046]: (a) for security-relevant circuits, the reverse engineering should be prevented such as preventing an erase of the data held in a memory chip upon the removal of the material that surrounds or covers the semiconductor chip since the passivation layer of the chip is, generally, accessible (e.g., via probing), (b) Examiner notes the protected data from erasing in the memory chip where the memory chip must comprise data / address buses to another part of electronic circuits that comprises a part of the connection means arranged for transferring data signals (i.e. as to be protected data) between those two electronic circuits; besides, (c) as per another connection means where the data signal conveyed on Figure 1 is also qualified as protected information since Laackmann teaches the signal receiver must receive approximately identical signal values from the transmitter (Para [0046]) and hence the conveyed signal level / information is normally protected unless an intrusion attack alters the signal value by changing the associated capacitance value).

a monitoring circuit arranged to monitor a deviation in the capacitance of the connection means and to generate an alert signal if the deviation exceeds a

predetermined value (Laackmann: Figure 1, Para [0002], Para [0005], Para [0012] and Para [0046]: (a) the change of capacitance can be detected and reported as a result of intrusive attack and (b) in the case of the capacitive associated measurement method, however, the signal receiver must receive approximately identical signal values).

As per claim 2, Laackmann teaches the monitoring circuit is arranged to monitor the data signals transferred via the connection means and to compare a monitored signal with a reference signal (Laackmann: Para [0046]: in the case of the capacitive measurement method, however, the signal receiver must receive approximately identical signal values).

As per claim 3, Laackmann teaches the electronic circuits comprise a logical circuit and a storage element arranged to store data output by the logical circuit (Laackmann: Para [0039] Line 9 – 13, Para [0004] Line 1 – 5 and Para [0003] Line 15 – 18) – Examiner notes, the memory chip as one side of electronic circuits must comprise a storage element such as part of the transistors as the component elements of a chip that comprise buffering circuits to buffer / store data-bit signal).

As per claim 6, Laackmann teaches the monitoring circuit is arranged to monitor a value of the capacitance of the connection means and to compare the monitored value with a reference value (Laackmann: Para [0046]: in the case of the capacitive measurement method, however, the signal receiver must receive approximately identical signal values).

As per claim 8, Laackmann teaches a dummy electronic circuit having at least a dummy connection means ith a capacitance comparable to that of the connection means, and wherein

the monitoring circuit is further arranged to determine the reference signal by monitoring the dummy connection means when transferring a data signal identical to that transferred via the connection means (Laackmann: Para [0047]: there are two measurements, namely, normal measurement method and capacitance measurement method, which are changed back and forth for a predetermined time interval and a different measurement signal must, then, correspondingly be received at the signal receiver in the case of the normal measurement method – Thereby, the capacitance measurement method is qualified as a dummy electronic circuit measurement with respect to the normal measurement method).

As per claim 9, Laackmann teaches the electronic device is further arranged to use the alert signal to power down at least a part of the electronic device (Laackmann: Para [0004]: an interruption or a short circuit attack is detected by an evaluation circuit that, then, directs the integrated circuit into a secure state which is triggering of <u>a reset or the erasure of the memory contents</u>).

As per claim 20, Laackmann teaches monitoring a capacitance of the connection means and comparing the capacitance of the connection means to a threshold (Laackmann: Para [0046]: an expected received measured signal identified as an approximately identical signal values is indeed qualified as a measurement value within a threshold).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art

to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 4 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laackmann et al. (U.S. Patent 2003/0132777), in view of Benkley (U.S. Patent 2003/0035570).

As per claim 4, Laackmann does not disclose expressly the monitoring circuit is a propagation delay detection circuit.

Benkley teaches the monitoring circuit is a propagation delay detection circuit (Benkley: Para [0090] / Last Para: the capacitance change can be evaluated as a time delay, which is also a well-known electric theory that capacitance time constant is related to the magnitude of the capacitance).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Benkley within the system of Laackmann because (a) Laackmann teaches providing a mechanism for protecting an integrated circuit against reverse engineering (e.g. probing) by using a method of capacitance associated measurement (Laackmann: Para [0012]), and (b) Benkley teaches the capacitance change can be evaluated as a time delay, which is also a well-known electric theory that capacitance time constant is related to the magnitude of the capacitance (Benkley: Para [0090] / Last Para).

As per claim 12, Laackmann as modified teaches the propagation delay detection circuit is configured to: perform a comparison of a plurality of signal values of the monitored signal with a plurality of signal values of the reference signal, and detect a propagation delay between the monitored signal and the reference signal based on the comparison of the signal values of the monitored signal and the reference signal (Benkley: Para [0090] / Last Para: unlike a discrete

digital signal, a propagation analog signal indeed comprises a time domain which constitutes a plurality of signal values).

9. Claims 5, 7, 13 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laackmann et al. (U.S. Patent 2003/0132777), in view of Rayane et al. ("A Digital BIST for Operational Amplifiers Embedded in Mixed-Signal Circuits" Proceedings of IEEE VLSI Test Symposium; 1999, pp. 304-310).

As per claim 5, Laackmann does not disclose expressly the monitoring circuit is a slew-rate deviation detection circuit.

Rayane teaches the monitoring circuit is a slew-rate deviation detection circuit (Rayane: Section 2.1).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rayane within the system of Laackmann because (a) Laackmann teaches providing a mechanism for protecting an integrated circuit against reverse engineering (e.g. probing) by using a method of capacitance associated measurement and transmitting a random or periodically changing signal sequence to the target (Laackmann: Para [0012] and [0047]), and (b) Rayane teaches providing an efficient technique of testing integrated circuit such as ASICs by using a slew-rate deviation detection method in the time domain (Rayane: Section 1 & 2.1).

As per claim 7, Laackmann does not disclose expressly the reference signal is derived from a Monte-Carlo analysis performed on the electronic device.

Rayane teaches the reference signal is derived from a Monte-Carlo analysis performed on the electronic device (Rayane: Section 4.1: Rayane teaches a Monte-Carlo analysis is

carried out to computer the variation of measurement due to tolerance – i.e. Examiner notes the expected measurement value (i.e. reference signal value) needs to consider / include the acceptable <u>tolerance</u> via the Monte-Carlo simulation as such the reference signal is indeed derived from a Monte-Carlo analysis).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rayane within the system of Laackmann because (a) Laackmann teaches providing a mechanism for protecting an integrated circuit against reverse engineering (e.g. probing) by using a method of capacitance associated measurement and transmitting a random or periodically changing signal sequence to the target (Laackmann: Para [0012] and [0047]), and (b) Rayane teaches providing a high accuracy technique of the test response analysis in order to computer the variation of measurements due to tolerances for integrated circuit – i.e. the expected measurement value (i.e. reference signal value) needs to consider the acceptable <u>tolerance</u> via the Monte-Carlo simulation (Rayane: Section 1 & 4.1).

As per claim 13 and 18, Laackmann as modified teaches performing a comparison of a plurality of signal values of the monitored signal with a plurality of signal values of the reference signal, and detect a slew-rate deviation between the monitored signal and the reference signal based on the comparison of the signal values of the monitored signal and the reference signal (Rayane: Section 1 & 2.1: unlike a discrete digital signal, a propagation analog signal indeed comprises a time domain which constitutes a plurality of signal values).

10. Claim 11 and 15 – 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laackmann et al. (U.S. Patent 2003/0132777), in view of Yamashita (U.S. Patent 6,467,083).

As per claim 11, Laackmann does not disclose expressly detection of a probe electrically coupled to the connection means, wherein the probe is electrically coupled to the connection means to gain unauthorized access to the protected information conveyed by the data signals.

Yamashita teaches detection of a probe electrically coupled to the connection means, wherein the probe is electrically coupled to the connection means to gain unauthorized access to the protected information conveyed by the data signals (Yamashita: Column 3 Line 63 – Column 4 Line 3: the trace controller and the trace memory controller are connected to the address bus and the data bus through a probe(s) and any probing coupled to the address bus and the data bus would increase the associated parasitic capacitance value which would result in the malfunction of the target system).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yamashita within the system of Laackmann because (a) Laackmann teaches providing a mechanism for protecting an integrated circuit against reverse engineering (e.g. probing) by using a capacitance measurement method so that the intrusion attack such as an erase of the data held in a memory chip can be detected when the associated capacitance measurement value varies as a result when the passivation layer of the chip become accessible by intrusion (Laackmann: Para [0012] Para [0012] and Para [0046]), and (b) Yamashita teaches any probing coupled to the address bus and the data bus would subsequently increase the associated parasitic capacitance and result in the malfunction of the target system (Yamashita: Column 3 Line 63 – Column 4 Line 3).

As per claim 15 – 17, see the similar rationale of rejections applying herein as set forth above in claim 11 – any probing coupled to the address bus and the data bus would increase

the associated parasitic capacitance value which would result in the malfunction of the target system. See the same rationale of combination applied herein in rejecting the claim 11.

11. Claims 14 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laackmann et al. (U.S. Patent 2003/0132777), in view of Benkley (U.S. Patent 2003/0035570), and in view of Rayane et al. ("A Digital BIST for Operational Amplifiers Embedded in Mixed-Signal Circuits" Proceedings of IEEE VLSI Test Symposium; 1999, pp. 304-310).

As per claim 14 and 19, the claim limitations are met as the same reasons as that set forth above in rejecting claim 4 and claim 5.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit ChaiPh.D
Primary Examiner, Art Unit 2431
02/10/2009